ANALYSES OF EUROPEAN CYBERSECURITY FRAMEWORKS

Maryna Yevdokymenko, Sebastian Floderus,
Linus Rosenholm, Vincent Tewolde
Kharkiv national university of radio electronics
(61166, Kharkiv, Nauky ave,14, V.V. Popovskyy department of
Infocommunication engineering, phone. (057) 702-13-20)

The main purpose of the paper is to analyze the EU cybersecurity frameworks and policies, to compare the development strategies of European countries and Ukraine, to identify compatibility and gaps between them for further developing recommendations for creating a more reliable and safe ecosystem through integrating EU cybersecurity frameworks.

EU is developing a suite of European cybersecurity standards that aim to deter and respond to cyber-attacks which constitute an external threat to the EU and its partner states by producing practices and guidelines on how to implement and enhance security, how to prevent attacks and provide cybersecurity hygiene. The European Cyber Security Organization (ECSO), European Union Agency for Cybersecurity (ENISA), IoT Security Foundation are the leading organizations for providing businesses, companies, and individuals with best practices in area of the security. Collectively, such organizations provide Frameworks for exchanging cybersecurity information between stakeholders as well as establish regulatory documents such as the EU Cybersecurity plan to protect open Internet and online freedom and opportunity, National Information Security (NIS) directives, Principles for IoT Security, standards in support of the Cybersecurity Certification, etc. While they represent the emerging common practice, such frameworks and regulatory documents are relatively new for the Ukrainian businesses and individuals.

The purpose of the paper is to provide of strategic documentation and cybersecurity approaches of the EU frameworks for exchanging cybersecurity information with further using of European experience in cybersecurity practices to the business, legal regulatory bodies, government institutes of Ukraine, as well as to the scientific and educational institutions.

Implementation of these EU cybersecurity frameworks will contribute to the creation of a single secure digital ecosystem. To do this, consider the main European frameworks for cybersecurity:

1. *Cybersecurity Strategy interlinks: European Agenda on Security's, Digital Single Market Strategy and Global Strategy*, which describe EU's cyber ecosystem, EU Cybersecurity Strategy and their goals.
2. *Cyber Defence Policy Framework*, which connected with EU's Cyber Defence Policy Framework, cyber defence capabilities, as well as the protection of the EU Common Security and Defence Policy (CSDP)

communication and information networks, Permanent Structured Cooperation Framework (PESCO) and EU-NATO cooperation.

3. *EU's Joint Framework on countering hybrid threats,* which connected with studying cyber threats to both critical infrastructure and private users, highlighting that cyberattacks can be carried out through disinformation campaigns on social media.
4. *Network and Information Security (NIS) Directive*, which connected with a blueprint for a quick and coordinated response to a major attack, and for the swift implementation of the NIS Directive.
5. *EU cybersecurity certification framework*, which connected with the creation of tailored and risk-based EU certification schemes, because certification plays a critical role in increasing trust and security in products and services that are crucial for the Digital Single Market.
6. *European Union Agency for Cybersecurity (ENICA)* as one of the most important organization for ensuring a high and effective level of network and information security within the Union, and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations

The main result of this paper is analyzing and comparing the development strategies of European countries and Ukraine, identifying compatibility and gaps between them and further developing recommendations for creating a more reliable and safe ecosystem through integrating EU cybersecurity frameworks.

References

1. https://ec.europa.eu/digital-single-market/en/cyber-security
2. Robert Ackerman. 2019. Too few cybersecurity professionals is a gigantic problem for 2019. Tech Crunch. Retrieved January 29, 2019 from https://techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019
3. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
4. S. N. Matheu, J. L. Hernandez-Ramos and A. F. Skarmeta, "Toward a Cybersecurity Certification Framework for the Internet of Things," in *IEEE Security & Privacy*, vol. 17, no. 3, pp. 66-76, May-June 2019. doi:10.1109/MSEC.2019.2904475